JOSEPH P. RUSSONIELLO (CSBN 44332)
United States Attorney

BRIAN J. STRETCH (CSBN 163973)
Chief, Criminal Division

ERIKA R. FRICK (CSBN 208150)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102
Telephone: (415) 436-6973
Facsimile: (415) 436-7234
Email: erika.frick@usdoj.gov

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. ARSENIO HUQUERIZA, Defendant.	No. CR 08-0119 PJH **UNITED STATES' RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS** Date: July 2, 2008 Time: 2:30 p.m.

The United States hereby files its response to defendant's motion to suppress physical evidence (*i.e.*, the child pornography seized from the defendant's residence pursuant to a search warrant executed on August 10, 2007). As set forth below, the defendant's motion to suppress should be denied in its entirety. Contrary to defendant's position, there is no requirement that agents serve a copy of the probable cause affidavit supporting the search warrant at the time of the search, so long as agents serve a copy of the warrant and the attachments delineating the items to be seized (as was done here). Moreover, the agents' decision – based on concerns for officer safety – to detain the defendant briefly in a patrol car while the residence was secured

was in full compliance with the Fourth Amendment.

An evidentiary hearing has not been scheduled in this case, and the government therefore does not plan to call any witnesses at the argument on this motion that is scheduled for July 2, 2008. Because there are no material facts in dispute, an evidentiary hearing is not required. Supplemental briefing after this Court hears this motion is also unwarranted. Defense counsel has now received a copy of the complete search warrant in this case and may present any remaining arguments in his reply to this response.

BACKGROUND

During the course of an investigation by the Bureau of Immigration & Customs Enforcement ("ICE"), ICE agents learned that the defendant, Arsenio Huqueriza, had used his PayPal account to purchase several subscriptions over the internet for access to child pornography websites. *See* Affidavit in Support of Search Warrant, attached hereto as Exhibit A, at ¶¶ 35-47. Based on that investigation, the government sought a search warrant for the defendant's residence, which they executed on August 10, 2007. During the search of the defendant's residence, agents found hundreds of photographs and videos containing child pornography. On February 28, 2008, the grand jury returned an indictment charging the defendant with one count of possessing child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B).

The details of the search on August 10, 2007 are provided in the Declaration of ICE Special Agent Ryan Hirt, attached hereto as Exhibit B. Prior to executing the search, Agent Hirt learned that the defendant is a retired San Francisco Police Officer and that he owned at least one firearm. Agent Hirt inferred that the defendant was familiar with police tactics and procedures and had received weapons training during his career. Based on those facts and circumstances, combined with the embarrassing nature of child pornography, he concluded that the defendant "posed a significant risk to officer safety." Exhibit B, ¶ 3.

On August 10, 2007, Agent Hirt, together with other ICE agents and two South San Francisco Police officers, served the federal search warrant at the defendant's residence. The

two police officers knocked at the front door at approximately 8:15 a.m. *Id.* ¶ 6. The defendant answered the door, and one of the officers asked him if he would come outside to discuss a reported traffic accident involving the defendant's red Dodge truck. *Id.* The defendant cooperated and took several steps out of the house. *Id.* At that point, the ICE agents – who had been waiting by the garage – identified themselves as federal agents and told the defendant that they were serving a search warrant on his residence. *Id.* The ICE agents advised the defendant that he was not under arrest, but that they needed to detain him while the residence was secured. *Id.* For officer safety reasons, the defendant was then handcuffed and placed him in the back of a police car for approximately 15 minutes. *Id.*

Once the residence was secured, the agents brought the defendant back into the downstairs of the residence and removed the handcuffs. *Id.* ¶ 9. Agent Hirt advised the defendant that he was not under arrest and that he was free to leave at any time. *Id.* Agent Hirt asked the defendant if he was willing to talk about the subject matter of the search, and the defendant declined to do so. *Id.* The defendant was shown a copy of the search warrant and attachments A, B, and C, which detailed the items to be seized as part of the warrant. *Id.* Agent Hirt did not provide the defendant with a copy of the probable cause affidavit of ICE Agent Brodie Allyn in support of the search warrant, which at that time was under seal. *Id.*

Agents seized two computer hard drives, VHS tapes, recordable compact discs, a Panasonic Palm Corner, and financial and miscellaneous documents. Agents also found, but did not seize, multiple firearms. *Id.* ¶ 13. After completing the search, the defendant was provided a full list of items seized, which was annotated on a property form, and a copy of the search warrant and attachments A, B, and C. *Id.* ¶ 13. Subsequent forensic analysis of the seized evidence revealed hundreds of images and video clips containing child pornography. *Id.* ¶ 14.

DISCUSSION

I. The Warrant Was Sufficiently Specific and Properly Served.

None of the defendant's challenges to the warrant itself has merit. The defendant claims that the affidavit is unsupported by probable cause and was never shown to the defendant, that

the warrant does not specify the things to be seized or persons or places to be searched with particularity, and that the warrant was not timely or properly served.

The warrant was supported by probable cause because, *inter alia*, agents had probable cause to believe that the defendant had purchased several child pornography website subscriptions using his PayPal account over the internet. *See* Exhibit A (affidavit). The defendant has not cast any doubt whatsoever on the facts supporting probable cause.

Nor does the fact that the affidavit demonstrating probable cause was not shown to the defendant at the time of the search affect in any way the legality of the search. The agents presented the defendant with a copy of the search warrant and also attachments A, B, and C describing the location to be searched and the items to be seized. Although the agents did not provide the sealed probable cause affidavit, they were not required to do so. Under *United States v. Celestine*, 324 F.3d 1095 (9th Cir. 2003), the Fourth Amendment does not require agents to serve the searched party with the probable cause affidavit when they execute a search. If, as here, "the face sheet and attachments clearly state that the agents have lawful authority to conduct the search and specify the location to be searched and the items sought, the affidavit supporting the probable cause determination need not be served at the time of the search." *Id.* at 1101.

II. The Agents' Brief Detention of the Defendant While Securing the Residence Complied with the Fourth Amendment.

The scope of the search was also lawful under the Fourth Amendment. The defendant claims that the search was "unreasonable or excessive in its scope," but the only argument he offers in support is his contention that the 15-minute detention of the defendant in handcuffs in the patrol car at the beginning of the search was excessive. Contrary to that claim, the short detention of the defendant to allow agents to secure the residence was entirely reasonable under well-established Fourth Amendment law.

In *Muehler v. Mena*, 544 U.S. 93 (2005), Iris Mena sued officers under 42 U.S.C. § 1983. She claimed that the officers had violated the Fourth Amendment by handcuffing her and

detaining her in a garage for two to three hours while they searched the attached residence pursuant to a warrant. The Supreme Court rejected that argument. The Court explained that "[a]n officer's authority to detain incident to search is categorical; it does not depend on the 'quantum of proof justifying detention or the extent of the intrusion to be imposed by the seizure.'" *Id.* at 98 (quoting *Michigan v. Summers*, 452 U.S. 692, 705 n.19 (1981)). The Court further ruled that "[i]nherent in *Summers'* authorization to detain an occupant of the place to be searched is the authority to use reasonable force to effectuate the detention." *Id.* at 98-99. The Court held that the two- to three-hour detention in handcuffs did not outweigh the government's continuing safety interests during a search of a gang house for dangerous weapons, despite the fact that Mena herself was not a suspect.

Under *Mena*, the detention in this case was clearly lawful. Although the safety concerns in this case may not have been quite as high as in *Mena*, the fact that the defendant was a former law enforcement officer known to have at least one weapon on the premises certainly created a justified concern for agent safety in conducting the search, and the 15-minute detention here was far less than the several hour detention in *Mena*. *See also Los Angeles County v. Rettele*, 127 S.Ct. 1989, 1992 (2007) ("In executing a search warrant officers may take reasonable action to secure the premises and to ensure their own safety and the efficacy of the search.") (quoting *Mena*, 544 U.S. at 98-100; internal quotation marks omitted).[1]

III. Neither an Evidentiary Hearing Nor Supplemental Briefing Is Warranted Here.

The defendant appears to assume that this Court's hearing of this motion on July 2, 2008 will be an evidentiary hearing with witnesses. It is undersigned counsel's understanding that this Court intended only to schedule oral argument on the motion for that date. In any event, the defendant has not established any need for an evidentiary hearing. "An evidentiary hearing on a motion to suppress need be held only when the moving papers allege facts with sufficient

[1] Nor is *Mena* limited to searches for contraband (as opposed to mere evidence). *See, e.g.*, *Dawson v. City of Seattle*, 435 F.3d 1054 (9th Cir. 2006) ("The doctrine of *Michigan v. Summers*, permitting police officers to detain individuals during a search, and the principle of [*Mena*], holding that the authority to detain incident to search is categorical, apply to all searches upon probable cause, not just to searches for contraband.").

definiteness, clarity, and specificity to enable the trial court to conclude that contested issues of fact exist." *United States v. Howell*, 231 F.3d 615, 620 (9th Cir. 2000). Here, there are no contested issues of fact. The attached affidavit of Agent Hirt, which describes the search, is entirely consistent with the defendant's account of the search. The only disputes are over whether the search was lawful, which as explained above, it plainly was. Thus, if the defendant does make a formal request for an evidentiary hearing, that request should be denied.

The defendant also requests an opportunity for supplemental briefing on this matter, "to address the testimony at that [evidentiary] hearing and the prosecution's arguments." Motion, at 5. That request should also be denied. Not only is there no evidentiary hearing currently set, at which such witnesses would be called, but also the defendant may make any remaining arguments in his reply to this response.[2]

DATED: June 4, 2008

Respectfully submitted,

JOSEPH P. RUSSONIELLO
United States Attorney

/s/

ERIKA R. FRICK
Assistant United States Attorney

[2] The defendant complains that the warrant "has not been provided to his attorney." Motion, at 3. Prior to this motion, defense counsel had not requested a copy of the warrant, which was under seal. In fact, to the best of undersigned counsel's recollection, the defense has never made any formal request for discovery. *See* Exhibit C (declaration of undersigned counsel). The defense has now been provided a copy of the affidavit and can make any remaining arguments in reply to this response.

EXHIBIT A

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

CR 08 3:07 -70473 JCS

IN THE MATTER OF THE SEARCH OF The Residence Located at: 696 Freesia Drive South San Francisco, CA 90480	**UNSEALING ORDER**

Good cause appearing therefor, it is hereby ordered that this entire case, including but not limited to, the Application and Affidavit for Search Warrant, the Search Warrant, all dated August 8 or 9, 2007, and all related papers in the above matter, be unsealed by the Clerk of the Court and become part of the public record.

DATED: 5/20, 2008

HON. EDWARD M. CHEN
United States Magistrate Judge

JOSEPH P. RUSSONIELLO (CSBN 44332)
United States Attorney

BRIAN STRETCH (CSBN 163973)
Chief, Criminal Division

ERIKA R. FRICK (CSBN 208150)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102
Telephone: (415) 436-6973
Facsimile: (415) 436-7234
Email: erika.frick@usdoj.gov

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN THE MATTER OF THE SEARCH OF The Residence Located at: 696 Freesia Drive South San Francisco, CA 90480	**No. CR 3-07-70473 JCS** **UNITED STATES' MOTION TO UNSEAL APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT AND SEARCH WARRANT**

The United States hereby moves this Court to unseal the Application and Affidavit for Search Warrant and Search Warrant in the referenced matter, all dated August 8 or 9, 2007. Upon motion of the government stating that the government believed that the disclosure of those documents might jeopardize the progress of the ongoing investigation described in the affidavit, the documents were sealed per Order of the Honorable Joseph C. Spero, dated August 8, 2007. The defendant has now been charged by indictment and is aware of the ongoing investigation. For those reasons, the government moves that this entire case be unsealed including, but not limited to, the motion to seal, application and affidavit for search warrant, and search warrant. The government requests that the foregoing

//

//

documents become part of the public record.

DATED: May 19, 2008

Respectfully submitted,

JOSEPH P. RUSSONIELLO
United States Attorney

ERIKA R. FRICK
Assistant United States Attorney

[redacted]

SCOTT N. SCHOOLS (SCBN 9990)
United States Attorney

DOUG SPRAGUE (CASBN 202121)
Acting Chief, Criminal Division

ERIKA R. FRICK (CSBN 208150)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102
Telephone: (415) 436-6973
Facsimile: (415) 436-7234
Email: erika.frick@usdoj.gov

Attorneys for Plaintiff

JCS

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

3 - 07 - 70473

IN THE MATTER OF THE SEARCH OF
The Residence Located at:

696 Freesia Drive
South San Francisco, CA 90480

UNITED STATES' APPLICATION TO SEAL APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT AND SEARCH WARRANT

[redacted]

The United States hereby moves this Court to seal the Application and Affidavit for Search Warrant and Search Warrant in the referenced matter for the reasons set forth in the Affidavit. The United States requests that the above-described materials be sealed to preserve the confidentiality of the ongoing investigation described in the affidavit. Accordingly, the United States respectfully requests that the Court grant the attached sealing order.

DATED: August 8, 2007

Respectfully submitted,

SCOTT N. SCHOOLS
United States Attorney

ERIKA R. FRICK
Assistant United States Attorney

SEALED BY ORDER OF COURT

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

JCS

3-07-70473

IN THE MATTER OF THE SEARCH OF
The Residence Located at:

696 Freesia Drive
South San Francisco, CA 90480

SEALING ORDER

UNDER SEAL

Good cause appearing therefor, it is hereby ordered that the Application and Affidavit for Search Warrant, the Search Warrant, and all related papers in the above matter, be filed and maintained under seal until further order of the Court.

DATED: 8/9, 2007

HON. JOSEPH C. SPERO
United States Magistrate Judge

SE[redacted]

AO 93 (Rev [illegible]) Search Warrant

UNITED STATES DISTRICT COURT

NORTHERN District of CALIFORNIA

In the Matter of the Search of
(Name, address or brief description of person or property to be searched)

A residence located at:
696 Freesia Drive
South San Francisco, CA 94080

SEARCH WARRANT

JCS

Case Number: 3-07-70473

FILED
AUG 13 2007
RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

TO: Brodie Allyn, Imm. & Customs Enforcement and any Authorized Officer of the United States

Affidavit(s) having been made before me by Brodie Allyn (Affiant) who has reason to believe

that on the person of, or ✓ on the premises known as (name, description and/or location)

A residence located at 696 Freesia Drive, South San Francisco, CA, and more particularly described in Attachment A, attached,

in the Northern District of California there is now concealed a certain person or property, namely (describe the person or property)

items described in Attachment B, attached,

I am satisfied that the affidavit(s) and any record testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before 8/17/2007 (Date)

(not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search ✓ in the daytime — 6:00 AM to 10:00 P.M. ~~I at anytime in the day or night as I find reasonable cause has been established and if the~~ person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to Hon. Joseph C. Spero, U.S. Magistrate Judge as required by law.

U.S. Magistrate Judge (Rule 41(f)(4))

Approved by Erika Frick, AUSA as to form

8/9/07 10:20 am
Date and Time Issued

at San Francisco, CA
City and State

Hon. Joseph C. Spero, U.S. Magistrate Judge
Name and Title of Judge

Signature of Judge

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The Subject Premises is located at 696 Freesia Drive, South San Francisco, California 94080. The Subject Premises is a two-story residence located on a cul de sac. The residence is light tan in color with a red tiled roof. The residence faces southwest and is on the northeast side of Freesia Drive. The residence is third from where the street ends in the cul de sac, and is located northwest of intersection of Freesia Drive and Orchid Drive. The numbers "696" appear in black on a white plastic sign located on the front of the residence. There is a black mailbox in front of the residence, as well as a yellow fire hydrant.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEARCHED FOR AND SEIZED

A. Images of child pornography and files containing images of visual depictions of minors engaged in sexually explicit activity and/or child pornography, in any form wherever it may be stored or found, including, but not limited to:

i. Any computer, computer system and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;

ii. Books and magazines containing visual depictions of minors engaged in sexually

explicit conduct, as defined in 18 U.S.C. § 2256;

iii. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

iv. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

B. Information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

ii. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

C. Credit card information including but not limited to bills and payment records;

D. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence; and

E. Records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

ATTACHMENT C

PROTOCOLS FOR SEARCHING ELECTRONIC DATA IN THE NORTHERN DISTRICT OF CALIFORNIA

1. In executing this warrant, the government must begin by ascertaining whether all or part of a search of a device or media that stores data electronically (collectively, the "device") that is authorized by this warrant reasonably can be completed at the site within a reasonable time. If the search reasonably can be completed on site, the government will remove the device from the site only if authorized by law because removal is (1) necessary to preserve evidence, or (2) if the item is contraband, a forfeitable instrumentality of the crime, or fruit of crime.

2. If the government determines that a reasonable search as authorized in this warrant cannot be completed at the site within a reasonable period, the government must determine whether all or part of the authorized search can be completed by making a mirror image of, or in some other manner duplicating, the contents of the device and then completing the search of the mirror image off site (e.g., at a computer crime laboratory).

3. The government may remove from the search location a device only if the device cannot be searched reasonably on site, or by mirror-imaging or otherwise duplicating its contents for off site examination – unless authorized by law to remove the device because (1) removing the device is necessary to preserve evidence, or (2) the device is contraband, a forfeitable instrumentality of the crime, or fruit of crime. The government also may remove from the site any related equipment (e.g., keyboards or printers) or documents (e.g., system operating or software manuals) that reasonably appear to be necessary to conduct an off-site search of a device in which data is stored electronically.

4. If the government removes a device or related equipment or documents from the place they were found in order to complete the search off-site, within ten (10) calendar days of the removal the government must file a return with a magistrate judge that identifies with particularity the removed device or related equipment or documents.

5. The government must complete an off-site search of a device that agents removed in order to search for evidence of crime as promptly as practicable, and in any event no later than thirty (30) calendar days after the initial execution of the warrant. Within thirty (30) calendar days after completing an off-site search of a device pursuant to this warrant, the government must return any device, as well as any related equipment or document that was removed from the site in order to complete the search, unless, under the law, the government may retain the device, equipment, or document (1) to preserve evidence, or (2) because the device, equipment, or document is contraband, a forfeitable instrumentality of the crime, or fruit of crime. Within a reasonable period, not to exceed sixty calendar days after completing the authorized search of a device, the government also must use reasonable efforts to destroy – and to delete from any devices or storage media or copies that it has retained or made – copies of any data that are outside the scope of the warrant but that were copied or accessed during the search process, unless, under the law, the government may retain the copies (1) to preserve evidence, or (2) because the copies are contraband, a forfeitable instrumentality of the crime, or fruit of crime. The deadlines set forth in this paragraph may be extended by court order for good cause shown.

6. In conducting the search authorized by this warrant, whether on site or off site, the government must make all reasonable efforts to use methods and procedures that will locate and expose only those categories of files, documents, or other electronically stored information that

are identified with particularity in the warrant while, to the extent reasonably practicable, minimizing exposure or examination of irrelevant, privileged, or confidential files.

7. The terms of this warrant do not limit or displace any person's right to file a motion for return of property under Fed. R. Crim. P. 41(g). Nor does the issuance of this warrant preclude any person with any interest in any seized item from asking the government to return the item or a copy of it.

8. The government must promptly notify the judge who authorized issuance of the search warrant (or, if that judge is unavailable, to the general duty judge) if a dispute arises about rights or interests in any seized or searched item – or any data contained in any searched or seized item – and that dispute cannot be resolved informally. The government must deliver a copy of this written notification to any person known to assert any such right or interest.

AO 93 (Rev. 12/03) Search Warrant (Reverse)

RETURN	Case Number: 3-07-70473	
DATE WARRANT RECEIVED 8/9/2007	DATE AND TIME WARRANT EXECUTED 0900 8/10/2007	COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT WITH

INVENTORY MADE IN THE PRESENCE OF
Special Agent Brodie Allyn, DHS - ICE

INVENTORY OF PERSON OR PROPERTY TAKEN PURSUANT TO THE WARRANT

Please See Attachments

CERTIFICATION

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

8/10/07
Diana Alvarez

Subscribed, sworn to, and returned before me this date.

Signature of Judge
JOSEPH C. SPERO

8/13/07
Date

SPECIAL AGENT IN CHARGE
U.S. CUSTOMS SERVICE
SAN FRANCISCO, CALIFORNIA

SEARCH WARRANT INVENTORY

DATE 08/10/07 TIME 8:30 LOCATION 696 Freesia Dr. CASE NO. SI07QR0JI0015 PAGE 1 OF 2 PAGES

So San Francisco CA

SUSPECT(S): HUQUERIZA, Arsenio

ITEM #	DESCRIPTION OF ITEMS SEIZED	LOCATION WHERE FOUND	FOUND BY
001	HARD DRIVE - Western Digital Serial# WD-WMAAT3076764	Room G in Dell	R Hirt
002	HARD DRIVE - Samsung - Serial# S01XJ20Y314270	Room H in Compaq Presario	R. Hirt
003	39 VHS	Room H	R Hirt
004	5 MINI VHS	" "	"
005	1 BLACK CD CASE w/ APPROX 50 CDs	" "	"
006	1 PANASONIC PV-L858 Palm Corder w/Cable SN HBWA31783	" "	"
007	135 Recordable CDs + DVDs	" "	"
008	2 Credit Card Statements	" "	"
009	4 Computer Printouts	" "	"

AH0015

SPECIAL AGENT IN CHARGE
U.S. CUSTOMS SERVICE
SAN FRANCISCO, CALIFORNIA

SEARCH WARRANT INVENTORY

DATE 08/10/07 TIME 0830 LOCATION 696 Freesia Dr. CASE NO SI07CR0251CRB PAGE 2 OF 2 PAGES
S. San Francisco, CA

SUSPECT(S): HUDUENZA, Arsenio

ITEM #	DESCRIPTION OF ITEMS SEIZED	LOCATION WHERE FOUND	FOUND BY
010	Handwritten Notes	Room H	HIRT

FILED

AO106 (Rev. 12/03) Affidavit for Search Warrant

UNITED STATES DISTRICT COURT

AUG X 9 2007

RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

NORTHERN DISTRICT OF CALIFORNIA

In the Matter of the Search of
(Name, address or brief description of person, property or premises to be searched)

A residence located at:
696 Freesia Drive
South San Francisco, CA 94080

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

Case Number: JCS

3-07-70473

I, Brodie Allyn being duly sworn depose and say:

I am a(n) Special Agent, Immigration & Customs Enforcement and have reason to believe
Official Title

that ☐ on the person of or ☑ on the property or premises known as (name, deseription and/or location)

A residence located at 696 Freesia Drive, South San Francisco, CA 94080, and more particularly described in Attachment A, attached,

in the Northern District of California

there is now concealed a certain person or property, namely (describe the person or property to be seized)

items described in Attachment B, attached,

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

believed to contain evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and/or property designed for use, intended for use, or used in committing a crime.

concerning a violation of Title 18 United States code, Section(s) 2252 & 2252A

The facts to support a finding of probable cause are as follows:

See attached affidavit of Brodie Allyn, incorporated herein by reference.

Continued on the attached sheet and made a part hereof: ☑ Yes ☐ No

Approved As To Form: AUSA Erika Frick

Signature of Affiant

Sworn to before me and subscribed in my presence,

8/9/07
Date

at San Francisco, CA
City State

Hon. Joseph C. Spero U.S. Magistrate Judge
Name of Judge Title of Judge

Signature of Judge

AH0017

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NORTHERN CALIFORNIA

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

IN THE MATTER OF THE SEARCH	)
OF THE RESIDENCE LOCATED AT:	)
	)
696 Freesia Drive	)
South San Francisco, CA 90480	)
	)

I, Brodie Allyn, Special Agent, being duly sworn, depose and state the following:

1. This affidavit is submitted in support of an application for a search warrant for the residence of Arsenio HUQUERIZA, which is located at 696 Freesia Drive, South San Francisco, CA 94080 (hereinafter referred to as the "Subject Premises"), and the computer(s) located therein, for evidence of violations of Title 18, United States Code, Sections 2252 and 2252A, as described more fully herein. The Subject Premises is more fully described in Attachment A, which is attached hereto and incorporated by reference herein.

2. The statements contained in this affidavit are based on my experience and training as a Special Agent and on information provided to me by other ICE agents, other law enforcement officers, and witnesses as part of this investigation. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. Rather, I have set forth facts that I believe are sufficient to establish probable cause to believe that the location to be searched contains evidence of violations of federal law as described more fully herein.

AGENT BACKGROUND

3. I am a Special Agent with U.S. Immigration and Customs Enforcement ("ICE"), Department of Homeland Security, and have been so employed since August of 2003. I am currently assigned to the Contraband Smuggling Group, San Francisco, California. Prior to my employment with ICE, I was employed as a Police Officer with the City of Howell, Michigan for approximately one year. I hold a Bachelor's degree from the University of Michigan. I also graduated from a certified Police Academy in Michigan, and was honorably discharged after serving as a United States Marine. I have received training in investigating violations of federal laws, including laws governing child exploitation and the possession, distribution, and receipt of child pornography. In the course of the investigation described herein, I have consulted with other federal agents, including other ICE agents who have written affidavits for or participated in the application for and execution of multiple search warrants over the course of their careers.

4. I am currently responsible for investigating violations of federal criminal statutes, including cases involving the sexual exploitation of children and material constituting child pornography. I have received training in techniques for investigating violations of Title 18, United States Code, including specifically 18 U.S.C. 2252(a)(1) and 2252(a)(4)(B) involving the transportation and possession of child pornography. In the course of the investigation described herein, I have consulted with other federal agents, including ICE agents at the San Francisco Airport, who have written affidavits for or participated in the application for and execution of multiple search warrants over the course of their careers.

SUMMARY

5. This investigation concerns alleged violations by Arsenio HUQUERIZA of 18 U.S.C. 2252 and 2252A, relating to material involving the sexual exploitation of minors. Based on my training and experience, and the facts described herein, I believe there is probable cause to believe that, during the time period from approximately September 2006 to June 2007, HUQUERIZA purchased access to member-restricted websites selling and distributing child pornography on at least three (3) occasions, totaling an investment of approximately $250 USD. Based on my training and experience, I believe there is probable cause that evidence of HUQUERIZA's illegal possession or use of child pornography or other illegal materials relating to the sexual exploitation of minors will be found at his residence, and in particular is likely to be found on any computers or computer items that are currently stored at his residence. Thus, based on all of the facts described herein, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of such criminal offenses may be located at the residence described in Attachment A, in violation of 18 U.S.C. 2252 and 2252A.

APPLICABLE LAW

6. 18 U.S.C. 2252 and 2252A prohibit a person from knowingly transporting, receiving, distributing, or possessing in interstate or foreign commerce, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct (child pornography). Based on the facts set forth below, there is probable cause to believe that the above-listed property contains evidence of criminal activity in violation of Section 2252(a)(1) (knowingly transporting or shipping in interstate commerce by any means a visual depiction involving the use of a minor engaging in sexually explicit conduct), Section 2252(a)(2) (knowingly receiving, distributing, or

reproducing in interstate commerce by any means a visual depiction involving the use of a minor engaging in sexually explicit conduct), Section 2252(a)(4)(B) (knowingly possessing any visual depiction that has been shipped or transported in interstate or foreign commerce by any means), and/or Section 2252A (knowingly mailing, transporting, shipping, or reproducing child pornography by any means in interstate commerce, or knowingly receiving, distributing, or possessing child pornography after it has been transported in interstate commerce by any means). The elements of the statutory violations for which there is probable cause to believe that HUQUERIZA committed one or more of those offenses are as follows:

a. the elements of 18 U.S.C. 2252(a)(1) are:

1. Defendant knowingly transported or shipped a visual depiction in interstate commerce by any means, including a computer;

2. the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct;

3. such visual depiction was of a minor engaged in sexually explicit conduct;

4. the defendant knew that such visual depiction was of sexually explicit conduct; and

5. the defendant knew that at least one of the persons engaged in sexually explicit conduct in such visual depiction was a minor.

b. the elements of 18 U.S.C. 2252(a)(2) are:

1. Defendant knowingly received a visual depiction that had been transported in interstate commerce by any means, including a computer;

2. the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct;

3. such visual depiction was of a minor engaged in sexually explicit conduct;

4. the defendant knew that such visual depiction was of sexually explicit conduct; and

5. the defendant knew that at least one of the persons engaged in sexually explicit conduct in such visual depiction was a minor.

c. the elements of 18 U.S.C. 2252(a)(4)(B) are:

1. Defendant knowingly possessed a visual depiction that had been transported in interstate commerce by any means, including a computer;

2. the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct;

3. such visual depiction was of a minor engaged in sexually explicit conduct;

4. the defendant knew that such visual depiction was of sexually explicit conduct; and

5. the defendant knew that at least one of the persons engaged in sexually explicit conduct in such visual depiction was a minor.

d. the elements of 18 U.S.C. 2252A are:

1. Defendant knowingly mailed, transported, shipped, or reproduced child pornography by any means in interstate commerce, or knowingly

received, distributed, or possessed child pornography after it had been transported in interstate commerce by any means, including a computer;

2. the production of such child pornography involved the use of a minor engaging in sexually explicit conduct;

3. such child pornography portrayed a minor engaged in sexually explicit conduct;

4. the defendant knew that such child pornography was of sexually explicit conduct; and

5. the defendant knew that at least one of the persons engaged in sexually explicit conduct in such child pornography was a minor.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachments B and C to this Affidavit:

8. "Child Pornography" includes the definition in 18 U.S.C. 2256(8), i.e., any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

9. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. 2256(5).

10. "Minor" means any person under the age of eighteen years. See 18 U.S.C. 2256(1).

11. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. 2256(2).

12. "Internet Service Providers" or "ISPs" are commercial organizations that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet, including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, (called "bandwidth") that the connection supports. Many ISPs assign each subscriber an account name, such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

13. "Domain Name" refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric

characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level (or "top-level") domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and, .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the worldwide web server located at the United States Department of Justice, which is part of the United States government.

14. "Log Files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

15. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

16. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

17. "Uniform Resource Locator" or "Universal Resource Locator" or "URL" is the

unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

18. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND REGARDING THE INTERNET

19. I have been formally trained in the investigation of crimes involving the sexual exploitation of children. I also own my own computer, have personal knowledge of the operation of a computer, and have accessed the Internet since 1996. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation,

I know the following:

20. The Internet is a worldwide computer network that connects computers and computer networks via high-speed data links and telephone lines for the purpose of communicating and sharing data and information. Connections between internet computers exist across state and international borders; therefore, information sent between two computers connected to the Internet frequently cross state and international borders even when the two computers are located in the same state. A user accesses the Internet from a computer network or Internet Service Provider ("ISP") that connects to the Internet. The ISP assigns each user an Internet Protocol ("IP") Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISPs employ dynamic IP addressing, that is, they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. The ISP logs the date, time, and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

21. Photographs and other images can be used to create data that can be stored in a computer. This storage can be accomplished using a "scanner," which is an optical device that can recognize characters on paper and, by using specialized software, convert them to digital form. Storage can also be captured from single frames of video and converted to an image file. After the photograph or other image has been scanned into the computer, the computer can store the data from the image as an individual "file." Such a file is known an image file. Computers are capable of displaying an image file as a facsimile of the original image on a computer screen.

22. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy or compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 250 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

23. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is stored in his computer. The process of transporting an image file to one's own computer is called "downloading." The user can then display the image file on his computer screen, and can choose

to "save" the image on his computer and/or print out a hard copy of the image by using a printer device (such as a lasercjet or inkjet).

25. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

THIS INVESTIGATION

Background Regarding "Home Collection" and Affiliated Websites That Advertise and Sell Child Pornography

26. In April 2006, Immigration and Customs Enforcement's Cyber Crimes Center, Child Exploitation Section, initiated an investigation into a criminal organization operating a commercial child pornography website known as "Home Collection." The "Home Collection" member-restricted website was located at URL: http://members.homecollect.us. The website offered individuals monthly access to a member restricted website for $79.95 a month. The member-restricted website communicated with customers via several different e-mail accounts.

27. The ICE investigation has further revealed that the same organization that operates "Home Collection" (hereinafter, the "Home Collection organization") is also operating numerous other commercial child pornography websites. ICE/C3/CES has conducted over 60 undercover transactions at approximately 23 different member-restricted websites that are affiliated with the Home Collection organization.

28. The Home Collection organization utilizes a payment website, www.iWest.com ("iWest"), to process payments for the various child pornography websites that the organization operates. The iWest website, in turn, redirects customers to PayPal[1] in order to complete payment.

Identification of PayPal Accounts Affiliated with the Home Collection Organization

29. Through this investigation, ICE determined that the Home Collection organization

[1]The following information was obtained from PayPal's website located at URL http://www.PayPal.com: founded in 1998, PayPal, an eBay Company, enables any individual or business with an email address to securely, easily and quickly send and receive payments online using a credit card or bank account information. PayPal identifies its accounts by the contact email address or addresses an

uses various PayPal accounts to process payments for the monthly subscription fees to its various member-restricted child pornography websites. PayPal, in turn, maintains transactional records for each PayPal account. The transactional records indicate at least the following information: date of purchase, time of purchase, name of customer, subject identifier assigned by the owner of the PayPal account indicating what the customer is purchasing, amount of purchase, customer's IP address, customer's e-mail address, seller's e-mail address, and the Item ID. In addition, PayPal also captures the customer's full billing address.

30. In order to determine which PayPal accounts the Home Collection organization was using, ICE agents conducted a number of undercover purchases following one of two below-listed patterns:

Pattern One:

i. The ICE agent accessed a website, affiliated with the Home Collection organization, that was advertising child pornography.
ii. The ICE agent was redirected to the "iWest" payment website and entered personally identifiable information, including credit card information. The "iWest" payment website identified a specific member restricted website through the use of the subject identifiers.
iii. After completing the required information and clicking "submit," the ICE agent was redirected to a second web page indicating the payment was currently being processed and to check for further information in the e-mail account provided by the ICE agent.
iv. The ICE agent received an e-mail containing instructions for completing payment, which included a hyperlink to a PayPal account.
v. The ICE agent completed the transaction via the PayPal account.
vi. The ICE agent received instructions for accessing the member-restricted child pornography website from one of the administrative e-mail addresses associated with the Home Collection organization.

---

account holder provides to PayPal as a contact address.

Pattern Two:

i. The ICE agent accessed a Home Collection organization-affiliated website advertising child pornography.
ii. The ICE agent was redirected to the "iWest" payment website, where the agent entered personally identifiable information, including credit card information. The "iWest" payment website identified a specific member restricted website through the use subject identifiers.
iii. After completing the required information and clicking "submit," the ICE agent was redirected to a second web page indicating the payment was currently being processed. The web page also contained a button the agent had to click to complete the payment.
iv. The ICE agent clicked the button and was redirected to a secure PayPal payment web page.
v. The ICE agent completed the transaction via the PayPal account.
vi. The ICE agent received instructions for accessing the member-restricted child pornography website from one of the administrative e-mail addresses associated with the Home Collection organization.

31. As described in the two patterns listed in paragraph 30, ICE agents that conducted the undercover transactions would enter personally identifying information at the "iWest" payment website, but would ultimately be redirected to PayPal to complete the transaction. Through the course of transactions conducted from approximately June 2006 to February 2007, ICE agents made undercover transactions for purchasing access to member-restricted child pornography websites and submitted payment to the following PayPal accounts (hereinafter, the "Suspect Merchant Accounts"):

Business Name:	**Primary E-Mail Address:**
Proof Soft	androdork@gmail.com
Lencomps LTD	lencomps@juno.com
Proof Soft	a_chakin@yahoo.com
Belfast LTD	belfastltd@juno.com
Belfast LTD	lag89@nc.rr.com
Financial Services	belfast_ltd@juno.com
Proof Soft	pallone21@gmail.com
Bullet Proof Soft	rrpay@hotmail.com
Bullet Proof Soft	Preyes1101@hotmail.com

Bullet Proof Soft	freeawh_bsb@yahoo.com
Bullet Proof Soft	bsb22flash@yahoo.com
Lencomps LTD	lencompsltd@juno.com
N/A	mr.corax@gmail.com
Jfire Financial	jufire@hotmail.com
A1_Soft_TM	webfs@email.com
S_Market	carbonnoid@hotmail.com

Identification of the Subject Identifiers and Item IDs Used in the PayPal Accounts

32. As discussed in paragraph 27, ICE agents have conducted over 60 undercover transactions during the course of this investigation, and those transactions have identified a group of PayPal accounts, the Suspect Merchant Accounts, that are being used to facilitate customer payments to specific child exploitation member restricted websites. ICE agents were able to obtain from PayPal the transactional logs from those Suspect Merchant Accounts.

33. Initially, the specific member-restricted child pornography websites could he identified in the PayPal transactional logs by the "subject identifiers" (i.e., names of the specific child pornography websites, such as "Home Collection") utilized by the Home Collection organization. In or about November 2006, the Home Collection organization stopped utilizing the listed subject identifiers to identify the specific member restricted websites associated with each purchase. Instead, they began using generic Invoice numbers, with a unique Invoice number assigned to each transaction. The criminal organization also assigned Item IDs to each of the specific member restricted websites. For each specific member restricted website, the criminal organization assigned a unique Item ID, which also appeared in the PayPal transactional logs.

34. The following subject identifiers with associated Item IDs were identified during undercover transactions:

Subject Identifier:	Item Number:
Sexy Angels	1000
Desired Angels	1001
Home Collection	1002
SickCR Package v5.06 Build 3638	1003
DarkRO XP Tools v2.04	1004
Underage Home	1005
Angel Collection 1006	1006
Angel Collection 1010	1010
HL Package/Hardlovers Paysite	1012
RH Collection	1013
Spycam Lolitas	1144
Boys Say Go	1156
Video Shop CD1	1159
Video Shop CD2	1160
Video Shop CD3	1161
Video Shop CD4	1162
Video Shop CD5	1163
Kidz Index	1177
CP City	1202
Lolivirgins	1192
Excited Angels	1218

Information Obtained Regarding Arsenio HUQUERIZA

35. ICE agents' analysis of the Suspect Merchant Accounts' transactional logs obtained from PayPal has provided the names and addresses of various customers, including the subject of this search warrant, Arsenio HUQUERIZA, who had purchased access to at least one of the identified child pornography websites. Using the Suspect Merchant Account transactional logs, ICE agents were able to determine the following:

36. On November 30, 2006, Arsenio HUQUERIZA made a payment to a PayPal account whose primary email was Preyes1101@hotmail.com, which refers to the business name Bullet Proof Soft (paragraph 33). The PayPal transactional logs provided the following relevant information about the November 30, 2006 transaction:

Date: November 30, 2006

Time: 20:34:36 PST
Gross: $94.95
From Email Address: arsenio@jps.net
Item ID: 1012
Referral URL:
http://suaxormtfmd.us/join/index.php?action=finish&id=18254&kcy=955ef69f73
09a881ad415062fb6fab7c
First Name: arsenio
Last Name: HUQUERIZA
Primary Email: arsenio@jps.net
Primary Address: 696 freesia dr. south san francisco CA, 94080 US

37. ICE agents determined from this transactional information that, on November 30, 2006, HUQUERIZA paid $94.95 through PayPal in order to purchase access to Item ID number "1012." During the course of this investigation, as explained above, ICE agents have identified specific Item Ids associated with child exploitation member restricted websites. As explained in paragraph 34, Item Id 1012 is otherwise known as "HL Package/Hardlovers Paysite," which is a member restricted child pornography website.

38. As ICE agents had learned from their undercover transactions, the "Hardlovers" website offered child pornography and contained the following sections: "Home;" "Updates;" "Pictures;" "Video;" "Site Support;" and "Logout." There were numerous galleries contained within the "Pictures" and "Video" sections. A partial capture of the member restricted website was obtained to include the entire subdirectory entitled "Baby" under the "Pictures" section. In addition, within the subdirectory "Girls" under the "Pictures" section images from the following two galleries were captured: "Sabban" and "Vicky." Several of the images depicted lascivious displays of the female minors' genitalia. In numerous images, the female minors were engaged in sexually explicit conduct with adult males. Approximately 1,980 of these images were submitted to NCMEC. Of those, NCMEC determined that 570 images depicted victims

previously identified by law enforcement investigations. The following image descriptions provide a sample of the content of the member restricted website:

Image kx04-03 (Inga)

(https://69.50.183.226:10000) (Baby/Gal09/kx04-03)

This image displays a nude prepubescent female minor. Her left hand is grasping an adult male's penis. Her right arm appears to be resting on the adult male's left leg.

Image lucy055 (Lucy)

(https://69.50.183.226:10000) (Baby/Lucy/lucy055)

This image displays a close up of a prepubescent female minor's vagina being penetrated by an adult male penis. There are two separate frames. The upper frame shows the adult male's hand pushing his penis into the female minor's vagina. The second frame shows the adult male's penis pushing against the female minor's vagina.

Image sabban52 (Sabban)

(https://69.50.183.226:10000) (Girls/Sabban/sabban52)

This image depicts a prepubescent female minor and a nude prepubescent male minor. The male minor is sitting in a chair. His left arm is draped across his stomach and his right arm is grasping the back of the female minor's head. The female minor appears to be kneeling on the floor with her right arm resting on the left thigh of the male minor. The female minor has the male minor's penis in her mouth.

39. In addition, as noted in paragraph 36, the PayPal transactional logs for HUQUERIZA's November 30, 2006 purchase contained a referring URL of: http://suaxormtfmd.us/join/index.php?action=finish&id=18254&key=955ef69f7309a881ad415062fb6fab7c. The "referring URL" reflects the website the customer was viewing immediately prior to connecting to the PayPal payment page. In other words, this information identifies the specific website that redirected the customer to a PayPal payment page. The National Center for Missing and Exploited Children ("NCMEC") was able to verify that the URL accessed by HUQUERIZA on November 30, 2006 contained child exploitation images.

40. After learning from the Suspect Merchant Account PayPal transactional logs that HUQUERIZA had made the above-described purchase on November 30, 2006 from the Hardlovers child pornography website, ICE agents issued a summons to PayPal for the transactional logs associated with HUQUERIZA's personal PayPal account, which had been used to make that purchase. On June 28, 2007, PayPal responded to that summons for account information related to HUQUERIZA. PayPal's response revealed that an active PayPal account was opened on September 28, 2006, in the name of Arsenio HUQUERIZA, with an address of the Subject Premises and an email address of arsenio@jps.net.

41. The records received from PayPal reflect that on September 28, 2006, HUQUERIZA purchased "HomeCollection 1001 20 days access," with an item number of "1001," which correlates to one of the other websites (Desired Angels) identified by ICE Agents as selling child pornography. The records further indicate that payment was made to "Belfast LTD" with an email address of "belfastltd@juno.com" (both of which are identified as associated with the Suspect Merchant Accounts, in paragraphs 33-34 of this Affidavit). For the

September 26, 2006 transaction, the PayPal account established by HUQUERIZA was billed $79.95.

42. The PayPal transactional logs for HUQUERIZA's personal PayPal account also confirmed a transaction on November 30, 2006. In this instance, HUQUERIZA purchased "Invoice #18254" with corresponding item number "1012". The payment was paid to "Bullet Proof Soft" with an email address of "PReyes1101@hotmail.com." For that transaction, HUQUERIZA's PayPal account was billed $94.95. As per the information provided in paragraphs 35-39, your affiant believes this transaction was a subscription to Hardlovers, one of the websites under investigation.

43. The PayPal records also indicate that a purchase occurred on June 4, 2007 at approximately 18:19 hours (PDT). In this instance, HUQUERIZA purchased item name "Invoice 78376" with corresponding item number "1199." The payment was paid to "JFire Financial" with an email address of "jufire@hotmail.com." As noted in paragraph 33, the PayPal account "JFire Financial" bearing email address "jufire@hotmail.com" was identified by ICE Agents as one of the accounts utilized for the payment for access to the suspect websites.

44. In addition, the above PayPal transaction records for the June 4, 2007 purchase also included the IP address HUQUERIZA made the purchase from, at approximately 18:19 hours (PDT). This IP Address, 69.181.245.70, is one controlled by Comcast Communications. On July 12, 2007, Comcast Communications' response to an ICE Summons revealed that from 0000 hours to 2359 hours PDT on June 4, 2007, that IP address was dynamically assigned to Aresenio HUQUERIZA's Comcast account. This account was created on May 10, 2005, is active, and is described by Comcast Communications as "Residential High Speed Internet

Service." Included in the response from Comcast was the service address for this account, which is the same as the address of the Subject Premises. Thus, the Comcast records serve as further confirmation that it was in fact HUQUERIZA who purchased a subscription to a website selling and distributing child pornography on June 4, 2007, and that HUQUERIZA does in fact reside at the Subject Premises.

45. A check with the California Department of Motor Vehicles indicated that an individual named Arsenio HUQUERIZA, with a date of birth of July 12, 1943, had been assigned California Driver's License Number A0307992. Under the address portion of the record appears the following, "San Francisco PD." Queries of Accurint yielded additional information for HUQUERIZA, including confirming his current address as the Subject Premises and that HUQUERIZA was a San Francisco Police Officer.

46. On June 27, 2007, your affiant observed a red 2000 Dodge Durango bearing license plate number 4JNY075 parked in front of the garage located at the Subject Premises. Per a query of the California Law Enforcement Telecommunications System (CLETS), that vehicle is currently registered to HUQUERIZA who resides at the Subject Premises.

47. On July 2, 2007, the United States Postal Inspections Service indicated that HUQUERIZA is currently receiving mail at the Subject Premises.

OFFENDER TYPOLOGY

48. Based on my previous investigative experience related to child pornography investigations, including investigations of subjects who subscribed to websites offering access to child pornography, I have learned that individuals who subscribed to such websites often have a sexual interest in children and in images of children, and who download images and videos of

child pornography. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings,

mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

INFORMATION REGARDING SEIZURE OF COMPUTERS

ICE's Need to Seize HUQUERIZA's Computer Items

49. Based upon my knowledge, training and experience, and the experience of other law enforcement personnel, I know that searches and seizures of evidence from computers commonly require agents to seize most of the computer items (hardware, software, and instructions), to be processed later by a qualified computer expert in a laboratory or other

controlled environment. That is almost always true because of the following:

50. Computer storage devices (like hard drives, diskettes, tapes, laser disks, Bernoulli drives and others) store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she may store it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This examination process can take weeks or months, depending on the volume of the data stored, and it would be impractical to attempt this kind of data search on-site.

51. Searching computer systems for criminal evidence is a highly technical process that requires expert skills to be applied in a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in some systems and applications. It is difficult to know before a search which expert should analyze the system and its data. A search of a computer system is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

52. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices, as well as the central processing unit ("CPU"). In cases like this one, where the evidence consists partly of graphic files, the monitor and printer are also essential to show the nature and quality of the graphic images that the system can produce. In addition, the

analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly retrieve the evidence sought.

53. In addition to being evidence of a crime, in cases of this sort, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, printer, modem and other system components were used as a means of committing offenses involving the sexual exploitation of minors in violation of law, and should all be seized on that basis alone. Accordingly, permission is sought herein to seize and search computers and related devices consistent with the scope of the requested search.

Northern District of California Computer Search Procedure

54. In executing this warrant, the government must begin by ascertaining whether all or part of a search of a device or media that stores data electronically (collectively, the "device") that is authorized by this warrant reasonably can be completed at the site within a reasonable time. If the search reasonably can be completed on site, the government will remove the device

from the site only if authorized by law because removal is (1) necessary to preserve evidence, or (2) if the item is contraband, a forfeitable instrumentality of the crime, or fruit of crime.

55. If the government determines that a reasonable search as authorized in this warrant cannot be completed at the site within a reasonable period, the government must determine whether all or part of the authorized search can be completed by making a mirror image of, or in some other manner duplicating, the contents of the device and then completing the search of the mirror image off site (e.g., at a computer crime laboratory).

56. The government may remove from the search location a device only if the device cannot be searched reasonably on site, or by mirror-imaging or otherwise duplicating its contents for off site examination – unless authorized by law to remove the device because (1) removing the device is necessary to preserve evidence, or (2) the device is contraband, a forfeitable instrumentality of the crime, or fruit of crime. The government also may remove from the site any related equipment (e.g., keyboards or printers) or documents (e.g., system operating or software manuals) that reasonably appear to be necessary to conduct an off-site search of a device in which data is stored electronically.

57. If the government removes a device or related equipment or documents from the place they were found in order to complete the search off-site, within ten (10) calendar days of the removal the government must file a return with a magistrate judge that identifies with particularity the removed device or related equipment or documents.

58. The government must complete an off-site search of a device that agents removed in order to search for evidence of crime as promptly as practicable and no later than thirty (30) calendar days after the initial execution of the warrant. Within thirty (30) calendar days after

completing an off-site search of a device pursuant to this warrant, the government must return any device, as well as any related equipment or document that was removed from the site in order to complete the search, unless, under the law, the government may retain the device, equipment, or document (1) to preserve evidence, or (2) because the device, equipment, or document is contraband, a forfeitable instrumentality of the crime, or fruit of crime. Within a reasonable period, not to exceed sixty calendar days after completing the authorized search of a device, the government also must use reasonable efforts to destroy – and to delete from any devices or storage media or copies that it has retained or made – copies of any data that are outside the scope of the warrant but that were copied or accessed during the search process, unless, under the law, the government may retain the copies (1) to preserve evidence, or (2) because the copies are contraband, a forfeitable instrumentality of the crime, or fruit of crime. The deadlines set forth in this paragraph may be extended by court order for good cause shown.

59. In conducting the search authorized by this warrant, whether on site or off site, the government must make all reasonable efforts to use methods and procedures that will locate and expose only those categories of files, documents, or other electronically stored information that are identified with particularity in the warrant while, to the extent reasonably practicable, minimizing exposure or examination of irrelevant, privileged, or confidential files.

60. The terms of this warrant do not limit or displace any person's right to file a motion for return of property under F.R.Cr.P. 41(g). Nor does the issuance of this warrant preclude any person with any interest in any seized item from asking the government to return the item or a copy of it.

61. The government must promptly notify the judge who authorized issuance of the search warrant (or, if that judge is unavailable, to the general duty judge) if a dispute arises about rights or interests in any seized or searched item – or any data contained in any searched or seized item – and that dispute cannot be resolved informally. The government must deliver a copy of this written notification to any person known to assert any such right or interest.

SPECIFIC ITEMS TO BE SEIZED

62. Based on my training and experience, together with the evidence I have reviewed in this investigation, I believe that visual depictions of minors engaged in sexually explicit conduct (as defined in 18 U.S.C. 2256) and stored in, related to, or originating from a computer, will be found in HUQUERIZA's residence. These items include, but are not limited to, the following:

A. Images of child pornography and files containing images of visual depictions of minors engaged in sexually explicit activity and/or child pornography, in any form wherever it may be stored or found, including, but not limited to:

i. Any computer, computer system and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to: visually depict child

pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;

ii. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256;

iii. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256; and

iv. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256;

B. Information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

ii. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as

defined in 18 U.S.C. § 2256;

C. Credit card information including but not limited to bills and payment records;

D. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence; and

E. Records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

REQUEST FOR SEALING

63. Because this investigation is continuing, disclosure of the search warrants, this affidavit and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, I request that the Court issue an order that the search warrant, the affidavit in support of application for the search warrant, the application for the search warrant and all attachments thereto be filed under seal until further order of this Court.

CONCLUSION

64. Based on the facts described above, I believe that, between approximately September 2006 and June 2007, HUQUERIZA purchased access to websites selling and distributing child pornography on at least three (3) occasions, totaling an investment of approximately $250 USD. Based on my training and experience, I believe that HUQUERIZA illegally possessed or used child pornography or other illegal materials at his residence. I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of such criminal offenses may be located at the residence described in

Attachment A, in violation of 18 U.S.C. 2252 and 2252A.

64. I, therefore, respectfully request that attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Special Agent Brodie Allyn
Immigration & Customs Enforcement

SUBSCRIBED and SWORN
before me this 10th of August 2007

Honorable Joseph C. Spero
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The Subject Premises is located at 696 Freesia Drive, South San Francisco, California 94080. The Subject Premises is a two-story residence located on a cul de sac. The residence is light tan in color with a red tiled roof. The residence faces southwest and is on the northeast side of Freesia Drive. The residence is third from where the street ends in the cul de sac, and is located northwest of intersection of Freesia Drive and Orchid Drive. The numbers "696" appear in black on a white plastic sign located on the front of the residence. There is a black mailbox in front of the residence, as well as a yellow fire hydrant.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEARCHED FOR AND SEIZED

A. Images of child pornography and files containing images of visual depictions of minors engaged in sexually explicit activity and/or child pornography, in any form wherever it may be stored or found, including, but not limited to:

i. Any computer, computer system and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;

ii. Books and magazines containing visual depictions of minors engaged in sexually

explicit conduct, as defined in 18 U.S.C. § 2256;

iii. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

iv. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

B. Information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

ii. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

C. Credit card information including but not limited to bills and payment records;

D. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence; and

E. Records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

ATTACHMENT C

PROTOCOLS FOR SEARCHING ELECTRONIC DATA IN THE NORTHERN DISTRICT OF CALIFORNIA

1. In executing this warrant, the government must begin by ascertaining whether all or part of a search of a device or media that stores data electronically (collectively, the "device") that is authorized by this warrant reasonably can be completed at the site within a reasonable time. If the search reasonably can be completed on site, the government will remove the device from the site only if authorized by law because removal is (1) necessary to preserve evidence, or (2) if the item is contraband, a forfeitable instrumentality of the crime, or fruit of crime.

2. If the government determines that a reasonable search as authorized in this warrant cannot be completed at the site within a reasonable period, the government must determine whether all or part of the authorized search can be completed by making a mirror image of, or in some other manner duplicating, the contents of the device and then completing the search of the mirror image off site (e.g., at a computer crime laboratory).

3. The government may remove from the search location a device only if the device cannot be searched reasonably on site, or by mirror-imaging or otherwise duplicating its contents for off site examination – unless authorized by law to remove the device because (1) removing the device is necessary to preserve evidence, or (2) the device is contraband, a forfeitable instrumentality of the crime, or fruit of crime. The government also may remove from the site any related equipment (e.g., keyboards or printers) or documents (e.g., system operating or software manuals) that reasonably appear to be necessary to conduct an off-site search of a device in which data is stored electronically.

4. If the government removes a device or related equipment or documents from the place they were found in order to complete the search off-site, within ten (10) calendar days of the removal the government must file a return with a magistrate judge that identifies with particularity the removed device or related equipment or documents.

5. The government must complete an off-site search of a device that agents removed in order to search for evidence of crime as promptly as practicable, and in any event no later than thirty (30) calendar days after the initial execution of the warrant. Within thirty (30) calendar days after completing an off-site search of a device pursuant to this warrant, the government must return any device, as well as any related equipment or document that was removed from the site in order to complete the search, unless, under the law, the government may retain the device, equipment, or document (1) to preserve evidence, or (2) because the device, equipment, or document is contraband, a forfeitable instrumentality of the crime, or fruit of crime. Within a reasonable period, not to exceed sixty calendar days after completing the authorized search of a device, the government also must use reasonable efforts to destroy – and to delete from any devices or storage media or copies that it has retained or made – copies of any data that are outside the scope of the warrant but that were copied or accessed during the search process, unless, under the law, the government may retain the copies (1) to preserve evidence, or (2) because the copies are contraband, a forfeitable instrumentality of the crime, or fruit of crime. The deadlines set forth in this paragraph may be extended by court order for good cause shown.

6. In conducting the search authorized by this warrant, whether on site or off site, the government must make all reasonable efforts to use methods and procedures that will locate and expose only those categories of files, documents, or other electronically stored information that

are identified with particularity in the warrant while, to the extent reasonably practicable, minimizing exposure or examination of irrelevant, privileged, or confidential files.

7. The terms of this warrant do not limit or displace any person's right to file a motion for return of property under Fed. R. Crim. P. 41(g). Nor does the issuance of this warrant preclude any person with any interest in any seized item from asking the government to return the item or a copy of it.

8. The government must promptly notify the judge who authorized issuance of the search warrant (or, if that judge is unavailable, to the general duty judge) if a dispute arises about rights or interests in any seized or searched item – or any data contained in any searched or seized item – and that dispute cannot be resolved informally. The government must deliver a copy of this written notification to any person known to assert any such right or interest.

EXHIBIT B

IN THE UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO, CA

UNITED STATES OF AMERICA, Plaintiff, v. ARSENIO HUGUERIZA, Defendant.	CRIMINAL NO. 08-0119 PJH DECLARATION OF ICE SPECIAL AGENT RYAN HIRT

I, Ryan Hirt, declare under penalty of perjury that the following is true and correct to the best of my knowledge and belief:

1. I am currently a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement (ICE). I have been so employed since 2006. As an ICE Special Agent, I am responsible for investigating violations of federal criminal statutes, including those involving the sexual exploitation of children and the production, possession, and distribution of child pornography. I have either participated in or have been the case agent of several child pornography investigations that have culminated to the level of probable cause for the issuance of search warrants. I have participated in the service of many such warrants, wherein ICE agents have been authorized by the District Court to enter into the residences of private individuals for the purpose of searching for and seizing evidence of child pornography.

2. In 2007, I was one of the case agents assigned to the matter of the United States v. Arsenio Huguerizo, CR-08-0119 PJH. The information contained in this declaration is known to me through a review of official reports created by other ICE agents, evidence seized, and through conversations with other ICE agents.

3. Through my investigation of Mr. Huquenza, I learned that he was a retired San Francisco Police Officer and owned a Smith and Wesson Model 59, 9MM revolver. Due to the fact that he was a former law enforcement officer, I believed that Mr. Huquenza was familiar with police tactics, procedures, and had received weapons training during his career. Based on this information combined with the embarrassing nature of child pornography investigations, I contended that when we served the search warrant on his residence Mr. Huquenza potentially posed a significant risk to officer safety.

4. On August 30, 2007, I and other ICE agents, assisted by two officers from the South San Francisco Police Department, served a federal search warrant for child pornography at the residence of Mr. Huquenza in South San Francisco, California. In an effort to minimize the risk to officer safety during the service of the search warrant, ICE Agent Brooke Allen requested that the police officers use a ruse to make initial contact with Mr. Huquenza.

5. At approximately 0815 hrs., I and the other ICE agents parked our vehicles down the street from Mr. Huquenza's residence. We approached his residence in a manner that concealed us from view from the front door of the residence. We stopped in a single file formation in front of the garage door and approximately six feet from the entryway to the front door of the residence. In this position, we were not in view of the front door. The front door is recessed from the entryway.

6. As we got in the position described above, the two uniformed South San Francisco Police Officers, driving a marked police car, parked and approached the residence from the opposite direction. The officers knocked on the front door of the residence at approximately 8:15 am. Mr. Huquenza answered the door and one of the officers asked him if he would come outside to discuss a reported traffic accident involving Mr. Huquenza's red Dodge truck. Mr. Huquenza cooperated with the officers and took several steps out of the threshold. Once we the ICE agents were in clear view of Mr. Huquenza, we identified ourselves as federal agents and told him we were serving a search warrant on his residence. We advised Mr. Huquenza that he was not under arrest but that we needed to secure him while the residence was secured. For officer safety reasons, Mr. Huquenza was handcuffed and placed in the back of the police car for approximately 15 minutes. The South San Francisco police officers accompanied Mr. Huquenza during this time.

While Mr. Huquenza was inside the police car, ICE agents entered the residence, announcing "Police with a search warrant" as they did so.

8. As ICE agents encountered Mr. Huquenza's family members inside the house, the family members were gathered in the family room, which is located on the second level of the house, immediately at the top of the stairs. Family members were not handcuffed, but were asked to remain in that area while agents conducted a protective sweep of the residence.

9. Once the residence was secured, ICE agents brought Mr. Huquenza back into the downstairs of the residence to separate from his family members to afford him a greater degree of privacy. I removed the handcuffs and again advised Mr. Huquenza that we were there to serve a search warrant. I advised him that the search warrant was for child pornography. I again told Mr. Huquenza that he was not under arrest and that he was free to leave at any time. I asked Mr. Huquenza if he was willing to speak with me about why we were there and Mr. Huquenza agreed to do so. Mr. Huquenza was shown a copy of the search warrant and Attachments A, B and C which described the place to be searched, detailed the items to be seized as part of the warrant and provided the Northern District of California computer search protocol. As is our practice and procedure for all search warrants that we execute, we did not provide Mr. Huquenza with a copy of the probable cause affidavit supporting the warrant.

10. During the time Mr. Huquenza was in the residence and I was speaking with him downstairs, one of the other ICE agents took photographs of each room in the residence. Once the photographs had been taken, agents began searching the rooms for evidence related to child pornography.

11. In the family room Mr. Huquenza's wife, adult son and daughter were advised that we were serving a search warrant and that they could leave at any time. Family members indicated they did not wish to leave, so agents asked them to remain in the upstairs family room. Mrs. Huquenza asked to wash her face and retrieve medication before; she was allowed to do so by agents. The son and daughter also asked to brush their teeth and were also allowed to do so. Whenever one of these requests was made, an agent of the same sex as the requester would accompany the family member.

12. During the course of the investigation and while in the upstairs family room, Mr. Huquenza's adult son and daughter freely conversed with agents about their future career interests, current college classes and other issues

execution of the search warrant. At one point, one of the agents retrieved a box of donuts from the kitchen and brought it to the family members. As the search of the residence continued, the family members asked if they could move from the upstairs area to the downstairs living room. At that time, the family was escorted to the living room, where they joined Mr. Huqueriza.

13. The on-scene investigation and search of the residence was completed at approximately 10:45am. It should be noted that multiple handguns were found in the residence, but none were seized. A total list of items seized by agents was annotated on a property form and given to Mr. Huqueriza along with a copy of the search warrant and Attachments A, B, and C.

14. Subsequent forensic analysis of the evidence seized from Mr. Huqueriza's residence revealed hundreds of images and video clips containing child pornography.

Date: June 4, 2008

[redacted]
Special Agent
Immigration and Customs Enforcement
San Francisco, CA

EXHIBIT C

JOSEPH P. RUSSONIELLO (CSBN 44332)
United States Attorney

BRIAN J. STRETCH (CSBN 163973)
Chief, Criminal Division

ERIKA R. FRICK (CSBN 208150)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102
Telephone: (415) 436-6973
Facsimile: (415) 436-7234
Email: erika.frick@usdoj.gov

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. ARSENIO HUQUERIZA, Defendant.	No. CR 08-0119 PJH **DECLARATION OF ASSISTANT UNITED STATES ATTORNEY ERIKA R. FRICK RE DEFENDANT'S MOTION TO SUPPRESS**

I, Erika R. Frick, declare under penalty of perjury that the following is true and correct to the best of my knowledge and recollection:

1. I am an Assistant United States Attorney in the Northern District of California and am counsel of record for the government in the above-captioned case.

2. The search warrant that was executed at defendant Arsenio Huqueriza's residence on August 10, 2007 was sealed by court order prior to its execution.

3. In his motion to suppress, the defendant complains that the warrant "has not been provided to his attorney." Motion, at 3. To the best of my recollection, prior to filing the instant motion, defense counsel David Butler had not requested from the government a copy of the

warrant, which was under seal. In fact, to the best of my recollection, defense counsel has never provided any letter to the government requesting any discovery in this case, nor is there any such letter in the government's file.

4. On Monday, June 2, 2008, I sent an e-mail to defense counsel asking him whether he had in fact submitted any letter to the government requesting discovery in this case. As of the signing of this declaration, I have received no response to that e-mail.

5. Shortly after the defendant's arraignment in the above-captioned case, I spoke with defense counsel and offered to provide a viewing of the child pornographic images at issue to defense counsel, but defense counsel has not followed up on that offer.

6. Upon receiving the defendant's motion to suppress, and after internal consultation about whether the search warrant could be safely unsealed, the government promptly sought to unseal the search warrant. The warrant was unsealed by order of the Honorable Edward M. Chen, U.S. Magistrate Judge, on May 20, 2008. The government provided a copy of the entire search warrant, including the probable cause affidavit, to defense counsel via facsimile on May 22, 2008.

DATED: June 4, 2008

ERIKA R. FRICK
Assistant United States Attorney